CSO
SECURITY AND RISK

From: www.csoonline.com

Network Security: The Basics

New to network security? Before you get lost in the bits and bytes, Stephen Northcutt of SANS provides a look at the essential concepts.

Stephen Northcutt, CSO

April 29, 2008

There are exactly two keys to information security or information assurance: first, **configure the system and network correctly** and keep it that way. Because this is impossible to do perfectly, the second key to information assurance is to **know the traffic coming into and out of your network**.[1] That way, if something terrible is happening you can detect it. Therefore, all the tasks that have to be done in network security break down into three phases or classes:

- Protection, where we configure our systems and networks as correctly as possible
- Detection, where we identify the configuration has changed or that some network traffic indicates a problem
- Reaction, after identifying quickly, we respond to any problem and return to a safe state as rapidly as possible

Defense in Depth

Because we cannot achieve perfect security we have to accept a certain level of risk. Risk is defined as the probability a threat will cross vulnerability. Risk is hard to calculate, but we get a rough idea by considering our attack surface, the exposure, and the reachable and exploitable vulnerabilities that we have. A vulnerability scanner or penetration test helps us measure or define our attack surface. One thing we do to lower our risk and improve our odds of survival is to use multiple defenses. There are five basic architectures to develop defense in depth.[2]

- The **uniform method of protection for defense-in-depth** generally involves a firewall separating the internal trusted zone from the Internet, most implementations have anti-virus in the mail store and forward on the servers and desktops. It generally means that all internal hosts receive the same level of protection from attack by the computer network infrastructure. It is the most commonly and easily implemented architecture and least effective in terms of achieving a high degree of information assurance unless all IT contained information assets are of equal importance to the organization.
- **Protected enclaves** simply means subdividing the internal network so that it is not one large zone without internal protections. This can be done with firewalls, VPNs, VLANS and Network Access Control.
- **Information Centric**. Adm. Grace Hopper, a famous early researcher in computing said, "Some day, on the corporate balance sheet, there will be an entry which reads, 'Information'; for in most cases, the information is more valuable than the hardware which processes it."[3] it is critical to understand and to be able to help others understand the value of information. In addition to richly valuable information such as intellectual property (patents, trademarks, copyrights, know how, data schema), there is also data

including the increasingly important business record. To build an information centric defense-in-depth architecture, we must locate our critical and valuable information and ensure the proper protections are in place. This used to be very costly and was avoided, but due to changes in the Federal Rules of Discovery, many organizations have to build process to locate all information and tag it, so this becomes much easier.

- **Threat Vector Analysis** defense-in-depth is similar to information centric; it requires us to identify the assets we want to protect in order of priority, perform an analysis to determine the paths the threat could use to reach the vulnerability and figure out how to place controls on the vectors to prevent the threat from crossing the vulnerability.
- **Role-based access control (RBAC)** is an access control method that organizations implement to ensure that access to data is performed by authorized users. Unlike other access control methods, role-based access control assigns users to specific roles, and permissions are granted to each role based on the user's job requirements. Users can be assigned any number of roles in order to conduct day-to-day tasks. For example, a user may need to have a developer role, as well as an analyst role. Each role would define the permissions that are needed to access different objects.[4] With Network Access Control we can extend this from groups on systems to the entire enterprise. It requires more configuration than protected enclaves, but it yields more protection.

Cryptography

When defense in depth fails, the only remaining protection for the data is cryptography. Cryptography is very strong: if your organization is using a modern algorithm, the encrypted information is so powerfully protected, the encrypted data cannot be attacked. However, the processes we use to manage the crypto keys can be attacked, so strong processes related to key management are a must. As an example, many organizations have purchased full disk encryption for their laptops. There is no way to reverse that encryption without the key. However researchers at Princeton recently demonstrated ways to capture the key from memory defeating the protection with many vendors products.[5] There are three types of cryptography algorithms: secret key, public key, and hash functions. Unlike secret key and public key algorithms, hash functions, also called message digests or one-way encryption, have no key. Instead, a fixed-length hash value is computed based on the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. The primary application of hash functions in cryptography is message integrity. The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or by other means. Hash algorithms are effective because of the extremely low probability that two different plaintext messages will yield the same hash value.[6]

Access, Authentication, Authorization

Sometimes called Triple A or AAA, these are the keys to implementing security in the organization. Access process should ensure the correct person is accessing your organizations computing and networking resources. Since passwords can be shared, many organizations use a physical token in addition to a password during the authentication process. Once authenticated, controls should be in place to make sure individuals only access the resources they are authorized to access.

Separation of Duties, Separation of Services

Separation of duties is a common policy when people are handling money so that fraud requires collusion of two or more parties. This greatly reduces the likelihood of crime. Information should be handled in the same way since it can be bought and sold easily. If your system administrators claim that their duties cannot be broken up, it is important to understand well run organizations do just that.[7] A long time ago, servers were so expensive that a single server would run multiple services. One of the lessons we learned from the first worm (malicious software that spreads by breaking into systems) was that if a server crashed with multiple services running on it we would lose the ability to supply all of those services. For the next ten years, it was considered good practice to have one service per machine; a mail server, a file server, and so forth. Today, with virtual machines and service oriented web architecture, we are moving back to multiple services, in fact far more services than before. This is fine as long as we factor in how to keep operating if something bad happens to that machine. There are

fields of study called continuity of operations, disaster recovery and business impact that provide insight into these fields of study.

Endpoint Security and Ubiquitous Computing

Wireless networking continues to grow, entire cities are connected with metropolitan wireless, if you have a PDA or advanced cell phone you are connected to the Internet at all times. These devices can communicate with your desktop or laptop computer via Bluetooth. Organizations are going to have to engineer security at the device itself, this is called endpoint security. It is no longer possible to believe in a security model where you are fairly safe because we are connected to a corporate LAN protected by a firewall and an intrusion prevention solution. Rather, we need to consider security in a ubiquitous computing paradigm, always on the Internet wherever we are.

Web, Web Browsers and AJAX

Odds are very high that your organization is spending a lot more money on webmasters, web programmers and the like than you were just five years ago. Most software application development is becoming focused on the web for delivery. This means that most of the information entering and leaving the majority of user computers is via the web. However, web browsers such as Internet Explorer were not purposely designed as security gateways. It is possible to attack a users computer via their browser. Until security becomes the most important priority for web browsing software, problems will continue to exist. This is going to be especially true with the new web 2.0 interfaces that use recently developed extensions to a programming language web browsers support called AJAX to deliver enhanced functionality, but at the cost of increased risk.

SOA and the Future

Web based programs are very complex to create and maintain because they potentially offer so much functionality. For instance, if you have an online stock trading account, you can research, trade, run financial reports and even do online banking. To manage complexity and make it possible to get product to market faster, organizations are learning to simply create atomic services. This is known as Service Oriented Architecture (SOA) and may one day be the primary tool to support mission critical applications. If your organization needs a service, it consults a directory called UDDI to find it. This is similar to using a search engine like Google, but programs do this without human intervention, at least that is the idea.

SOA offers and exposes more business logic than a regular web server, after all each and every service you offer has to be in the directory if you want client programs to find you. A big part of the security battleground of the future will be centered around SOA, limiting the unauthorized release of sensitive information and creating gateways and other tools to protect the services. ##

Former CISO Stephen Northcutt is President of The SANS Technology Institute and co-author of Inside Network Perimeter Security (2nd Edition) (Inside)and the IT Ethics Handbook: Right and Wrong for IT Professionals.

1 http://www.sans.edu/resources/securitylab/pari_networks_kumar.php
2 http://www.sans.edu/resources/securitylab/76/
3 http://womenshistory.about.com/od/quotes/a/grace_hopper.htm
4 http://www.sans.edu/resources/student_projects/200608_002.doc
5 http://citp.princeton.edu/memory/
6 http://www.sans.edu/resources/securitylab/hash_functions.php
7 http://www.sans.edu/resources/securitylab/it_separation_duties.php

http://www.csoonline.com/article/342820/network-security-the-basics
http://www.csoonline.com/article/print/342820